IP Service Manager User Guide

Infrastructure Client for ISM Provision

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: April, 2002
Part number: 100121-00 rev 01

©2002 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Alpine, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS, and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodrive logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

All other registered trademarks and service marks are property of their respective owners.

Contents

Preface

Introduction vii
Terminology viii
Conventions viii
Related Publications x

1 Infrastructure and Services Management Provision Overview

Overview 1-1
Summary of Features 1-2
How ISM Provision works 1-3
Your Network Devices 1-4
ISM Provision Server 1-4
Device Communicators 1-4
Network Infrastructure Manager Client 1-5
IP Service Manager Client 1-5

2 Starting IP Service Manager

Overview 2-1
Starting IP Service Manager 2-1
Summary Steps 2-1
Detailed Steps 2-2

3 IP Service Manager Overview

IPSM Overview 3-1
- Summary of Features 3-1
- IPSM Views 3-2
  - Selecting IPSM Views 3-2
  - Service Activation View 3-4
  - Service Library View 3-5
  - Change Control View 3-6
- IPSM Icons 3-6
  - Open Changes 3-7
  - Save Changes 3-7
  - Modify Object 3-7
  - Copy 3-7
  - Paste 3-7
  - Delete 3-7
  - Verify Configuration 3-8
  - Synchronize 3-8
  - Commit Changes 3-8
  - Revert Changes 3-8
  - Help 3-8

4 Service Library

Overview 4-1

Traffic Policies 4-2

Policy Based Services 4-2

Service Bundles 4-2

Service Categories 4-3

Key Information 4-3

Service Library Tasks 4-3
- Add a Service Bundle 4-4
- Add a Policy Based Service 4-7
- Add an IP, TCP or UDP Traffic Policy 4-9

5 Service Activation

Overview 5-1

Subscriber 5-2

Customer 5-2

IP Aggregation Point 5-2

Service Activation Tasks 5-2
- Add a Customer 5-3
- Add an IP Subscriber 5-7
- Add an IP Range Subscriber 5-9
- Add an IP Aggregation Point 5-12

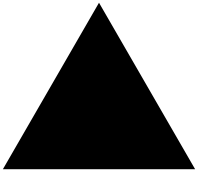
6 Change Control

Overview 6-1

Jobs 6-1

Change Control Tasks 6-2
- View Current Job Changes 6-2
- View Committed, Scheduled, or Saved Jobs 6-4
- Delete Scheduled or Saved Jobs 6-6

Index



Preface

This Preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the required information to manage customers and subscribers using Extreme Networks' IP Service Manager (IPSM) client as the interface for Extreme Networks' Infrastructure and Services Management Provision (ISM Provision).

This guide is intended for use by network administrators who are responsible for configuring network equipment. It assumes a basic working knowledge of:

- Local area networks (LANs).
- Ethernet concepts.
- Ethernet switching and bridging concepts.
- Routing concepts.
- Internet Protocol (IP) concepts.
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- Simple Network Management Protocol (SNMP).

Additionally, this guide assumes a familiarity with the features and functionality of ExtremeWare Software and with Extreme Networks' hardware. See the section, "Related Publications", for documents covering Extreme Networks' Software and Hardware.

If the information in the release notes shipped with your software differs from the information in this guide, follow the release notes.

Terminology

When features, functionality, or operation is specific to the Summit, Alpine, or BlackDiamond switch family, the family name is used. Explanations about features and operations that are the same across all Extreme switch product families simply refer to the product as the “Extreme device” or “Extreme switch.” Explanations about features that are the same for all devices managed by Network Infrastructure Manager (both Extreme devices and others) simply refer to “devices.”

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
`Screen displays bold`	This typeface indicates how you would type a particular command.

Table 2: Text Conventions (continued)

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in **Bold** type	GUI elements are written in bold type. Example: the menu item **File>Open**, the **Browse** button, the **Password** field name
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used to denote variables, such as VLAN names, or user account names.

Related Publications

The publications related to this one are:

- *ISM Provision Installation Guide*
- *Network Infrastructure Manager User Guide*
- *ExtremeWare Software User Guide*

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

http://www.extremenetworks.com/

1 Infrastructure and Services Management Provision Overview

Overview

Extreme Networks' Infrastructure and Services Management Provision (ISM Provision) is a tightly connected collection of components for delivering services to customers and for managing your network. ISM Provision allows you to easily extend services to your network users by defining and provisioning bundles of IP services. Services are managed as simple objects that are easy to apply to customers, but the configuration changes required to support the delivery of services is managed by ISM Provision. ISM Provision also allows you to control all or a portion of your network, by controlling the configurations of the devices in the network.

ISM Provision is designed to make it much easier to roll out changes to the network. You can add devices and make configuration changes offline and apply them to your network later. Planned changes are verified against a comprehensive set of rules to assure that the changes can be applied to your network and will not conflict with existing configurations. Incomplete sessions can be saved to be completed later.

Services provided across a group of customers can be easily modified. Once a service is updated, the change is applied to all customers using the service. ISM Provision manages all the configuration changes to make the modifications.

Network Infrastructure Manager (NIM) is the GUI client portion of ISM Provision that controls and manages the infrastructure of your network, the configurations of your network devices. NIM works closely with IP Service Manager (IPSM), the GUI client portion of ISM Provision that allows a provider to manage customers, service bundles, and policy based services.

Summary of Features

- Version Control of Network Configuration
- Staging of Network Configuration Changes
- Configuration rules checking
- Helps Manage the VLANs, Access Lists, and QoS Profiles Required to Support Subscribers
- Provides Service-Level Abstractions to Manage Subscribers
- Client/Server Java architecture - platform independent and scalable
- Offline and on-line tool - used in both green field and existing network environments
- Co-exists with other management tools using CLI or SNMP
- Version control for configurations and deployment module for system rollouts
- Provides an abstraction model that simplifies and automates both infrastructure and subscriber provisioning life-cycles
- Distributed device communication infrastructure for redundancy and scaling

How ISM Provision works

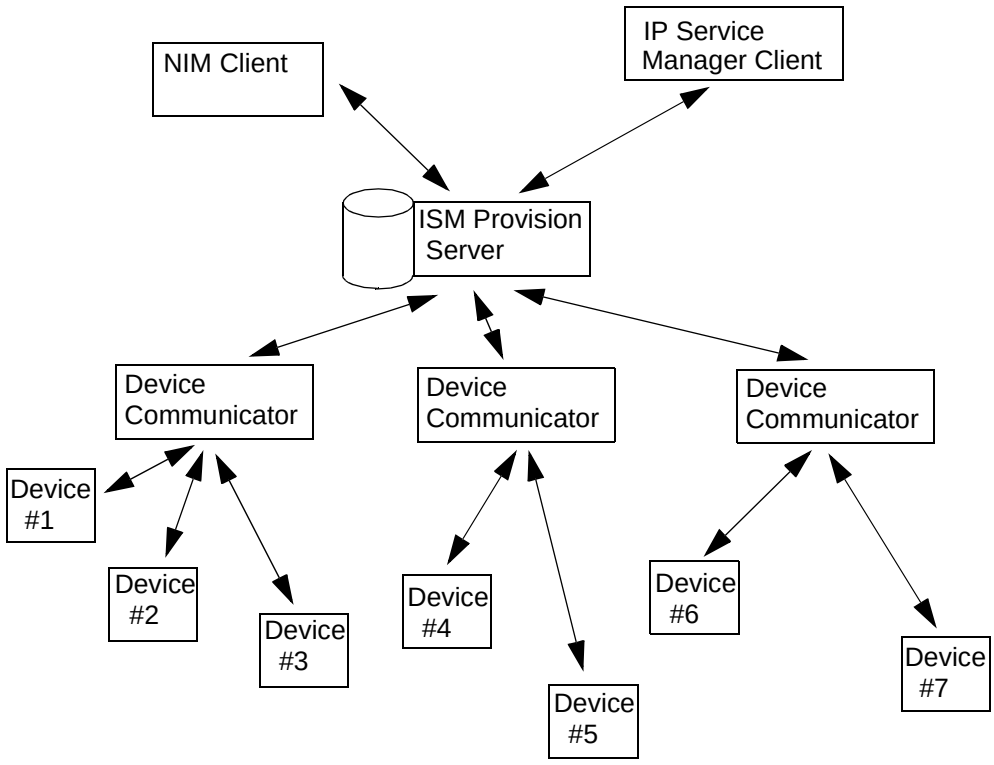


Figure 1-1: ISM Provision Components

ISM Provision consists of several different components:

- ISM Provision Server
- Device Communicators
- Network Infrastructure Manager Client
- IP Service Manager Client

These components work together to manage another important component:

- Your Network Devices

The following sections describe these components and how they interact in more detail.

Your Network Devices

The network managed by ISM Provision consists of your current existing network of Extreme Network devices, or a subset of your devices. Many devices can be managed by ISM Provision simultaneously. The devices are managed by querying them for their configurations, and by sending new configuration commands to them. Once ISM Provision manages a device, it will periodically check that the device configuration for changes.

ISM Provision Server

The ISM Provision server is the heart of ISM Provision. You may have more than one instance of the other components, but only one server. The server contains the information about the configurations of the managed devices, configurations that are scheduled to be applied to the network at a later time, and previous configurations. An ISM Provision server can contain the configurations of a large number of devices, but does not communicate with the devices directly. Instead, it uses device communicators to handle this task.

The ISM Provision server also contains the saved configuration changes that have not yet been applied to the network. These changes may be saved to edit later, or may be applied at a future time to the network.

Device Communicators

The device communicators control the communication between the network devices and the ISM Provision server. All queries to devices from the ISM Provision server and all commands from the ISM Provision server to the devices are handled by the device communicators. To spread the processing load across hosts, there can be more than one device communicator in an ISM Provision installation, but only one per host.

For example, in a network of 100 devices all managed with the same ISM Provision server, you might have five different device communicators, each talking with twenty devices. Any one managed device can only be managed by one device communicator, otherwise conflicts will occur.

Typically, you will install one device communicator on the same host as the ISM Provision server, and then add other device communicators on other hosts as needed to manage the processing load of communicating with your devices.

Network Infrastructure Manager Client

The Network Infrastructure Manager (NIM) client is used to manage changes to the network infrastructure. With NIM you can prepare and commit changes to the current network configuration, and add new devices to be provisioned. Before changes are rolled out to your network, NIM tests your proposed changes against a set of rules designed to spot and help you correct errors (for example, duplicate IP addresses assigned to different VLANs).

The NIM client also manages the providers, provider accounts, and provider access to network resources. With NIM you can define a provider and restrict that provider's control to a specific set of ports on a specific set of devices. You can also restrict the allowable VLAN IDs and IP addresses that the provider can assign.

The NIM client also manages the ISM Provision server and device communicators. You can see the status of the server and communicators and examine their logs. You can also see who is currently connected to the ISM Provision server and send a broadcast message to them. You can shutdown the ISM Provision server from within NIM.

Finally, you can review the current changes in your session, review committed, saved and scheduled jobs, and perform configuration versioning.

IP Service Manager Client

The IP Service Manager client allows providers to manage subscribers (subscribers consist of a VLAN and a single port in your network). IP Service Manager also allows you to configure service bundles (these correspond to QoS profiles) and policy based services (these correspond to access control lists) for these subscribers.

2 Starting IP Service Manager

Overview

Since the IP Service Manager (IPSM) client is part of ISM Provision, IPSM relies on a running ISM Provision server and device communicator. This chapter assumes that you already have a functioning ISM Provision server and device communicator.

Starting IP Service Manager

The following is a short summary of the steps to start IP Service Manager

Summary Steps

To start IP Service Manager you must:

1. **Launch the IPSM Client**
2. **Specify the ISM Provision Server**
3. **Enter your Provider Name**
4. **Enter a User Account Name**
5. **Enter the Password for the Account**

Detailed Steps

1 Launch the IPSM Client

Launch the IPSM client as you would launch other applications on your host. For example, Windows users can select Network Infrastructure Manager from the **Start>Programs>Extreme Networks>ISM Provision>Applications** menu. Solaris users can launch the **ipsm** executable file from the **/opt/extreme/ismprov/bin** directory by using a graphical file manager application to double-click on its icon, or by typing:

```
/opt/extreme/ismprov/bin/ipsm
```

Once the application starts, you will see the login screen similar to the one shown in Figure 2-1.

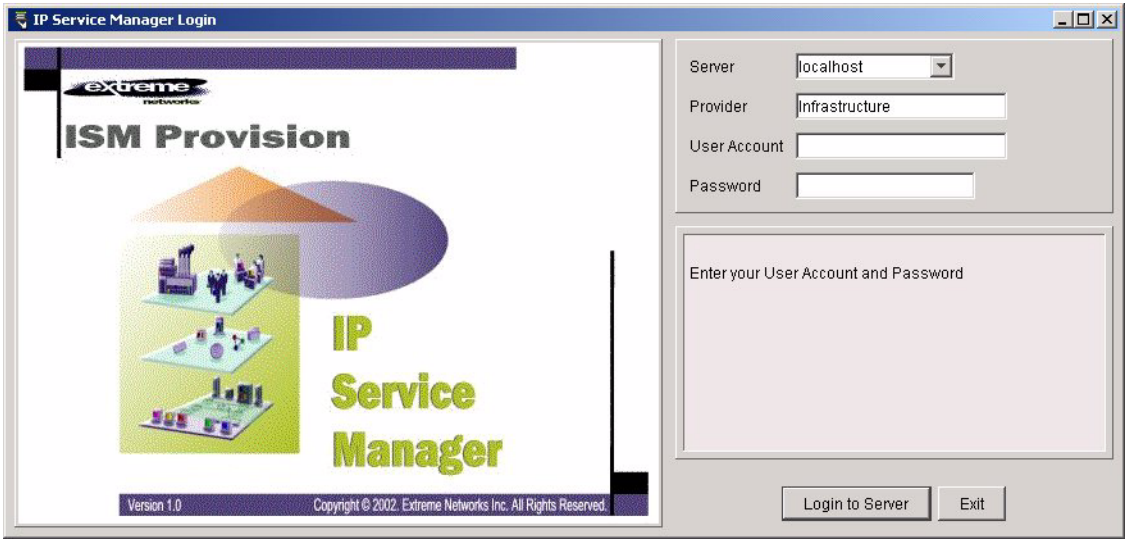


Figure 2-1: IP Service Manager Login Screen

2 Specify the ISM Provision Server

Once the login screen appears, you will specify the ISM Provision server. Specify the IP address of the server or the hostname by typing it into the server field. Figure 2-2 shows the login screen and server field in more detail.

IPSM will store the IP addresses and names that you have specified in previous sessions, so you may find your server already specified, or you may be able to select it from the drop-down list in the server field. Click on the down-arrow on the right side of the field and select the server.

Figure 2-2: IPSM Login Screen Detail

3 Enter your Provider Name

In the **Provider** field, enter the name of the provider that you belong to. If you have previously used IPSM, you will find the previous provider name already entered.

4 Enter a User Account Name

In the **User Account** field, enter your user account name.

5 Enter the Password for the Account

In the **Password** field, enter the account password. The account passwords are not saved and will need to be entered every session.

Once the information has been entered, the IPSM client will attempt to connect with the ISM Provision server. While it is connecting you will see messages similar to those in Figure 2-3.

Figure 2-3: The IPSM Client Connecting to the ISM Provision Server

Once the IPSM client is launched, you will see the **Service Activation** view.

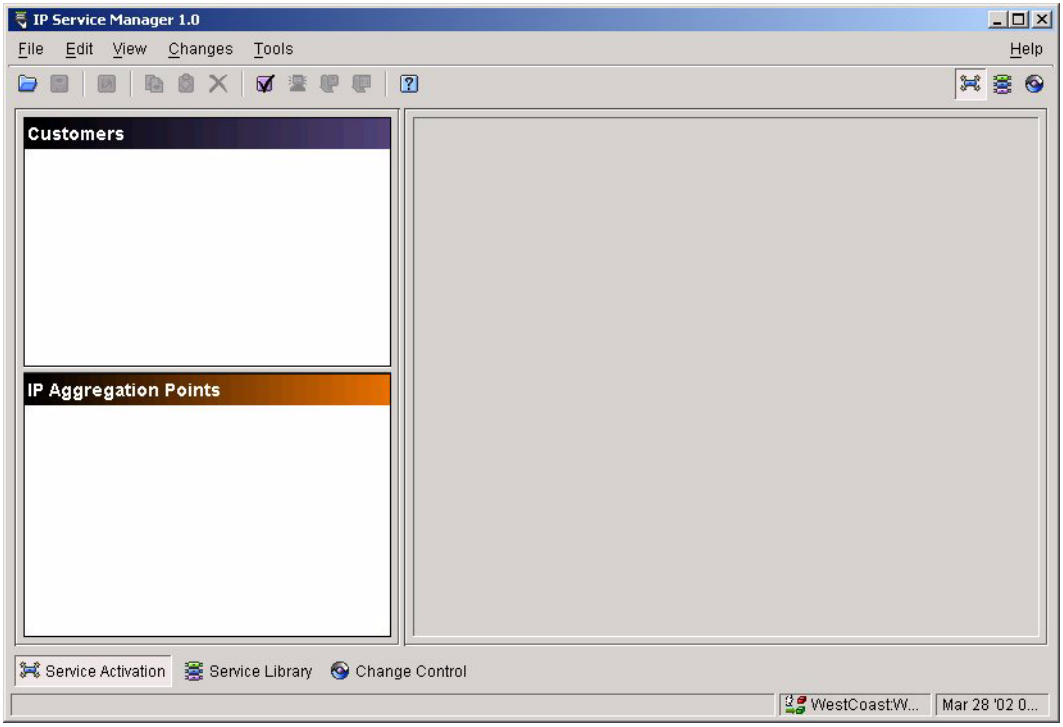


Figure 2-4: IPSM Initial Screen

When IPSM launches, the **Service Activation** view is initially displayed. You are now ready to use IPSM. See Chapter 3, *IP Service Manager Overview*, for more information about IP Service Manager.

3 IP Service Manager Overview

IPSM Overview

IPSM is composed of a number of views that are organized to complement your workflow. The different views allow you to manage different functional areas controlled by IPSM. They are:

- Service Activation View
- Service Library View
- Change Control View

IPSM also has a number of icons and menus that are available from all of the views.

Summary of Features

- Network partitionable for multiple Service Providers - restrictions to network resources
- IP Subscriber, service and traffic policy abstractions to hide configuration complexity
- Service template library for quick additions / modifications to a service or service bundle
- Transaction-oriented service activation and change management

IPSM Views

When IPSM is first launched you will be presented with the **Service Activation** view, as shown in Figure 3-1. The different views are described below.

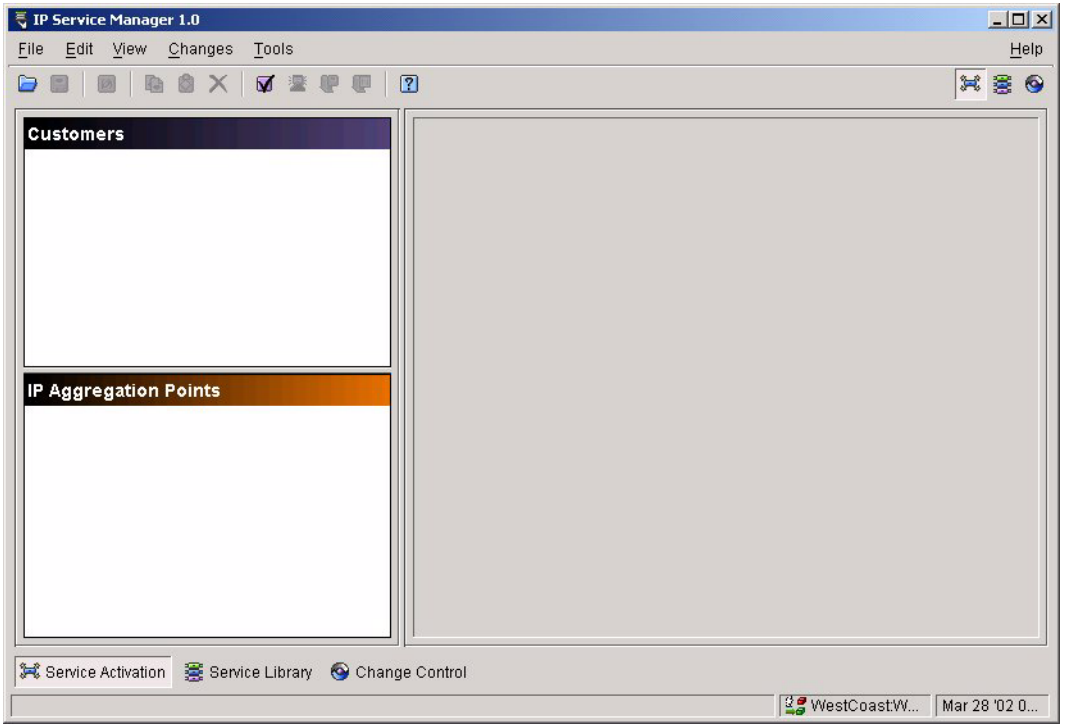


Figure 3-1: Initial IPSM Initial Screen

Selecting IPSM Views

There are four ways to select a particular view. One way is to select the desired view from the icons near the upper right side of the IPSM client screen, as shown in

Figure 3-2. From left to right the icons represent the views **Service Activation**, **Service Library**, and **Change Control**. Select the icon to display the view.

Figure 3-2: Selecting a IPSM View Using Icons

A second way is to select the **View** menu and choose the view, as shown in Figure 3-3. A third way is to use the shortcut keys also shown in Figure 3-3. Press the [ALT] key and a number key at the same time to use the shortcuts. For example, press [ALT]+3 to choose the **Change Control** view.

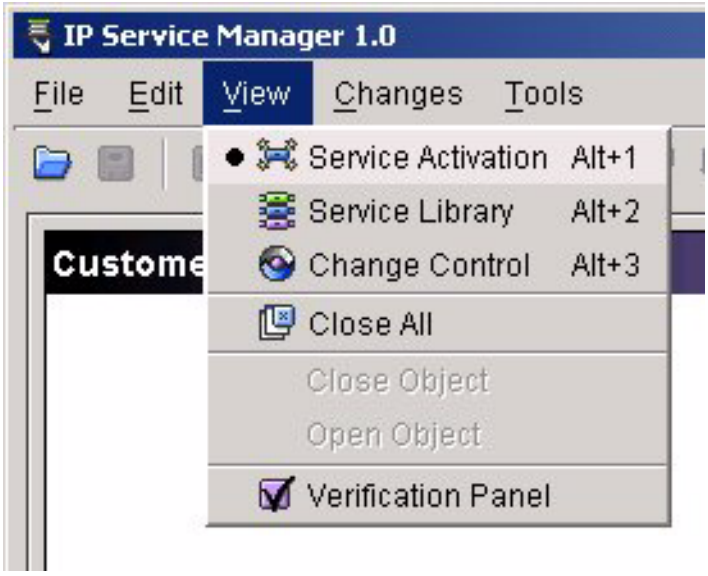


Figure 3-3: Selecting an IPSM View Using the Menu

A fourth way is to select the view from the named icons near the bottom of the IPSM client screen, just above the status line, as shown in Figure 3-4.

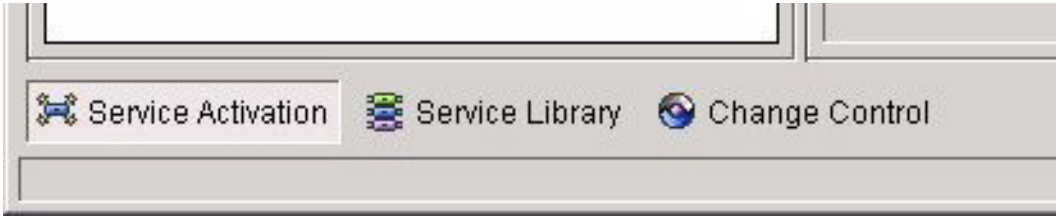


Figure 3-4: Selecting an IPSM View Using Named Icons

Service Activation View

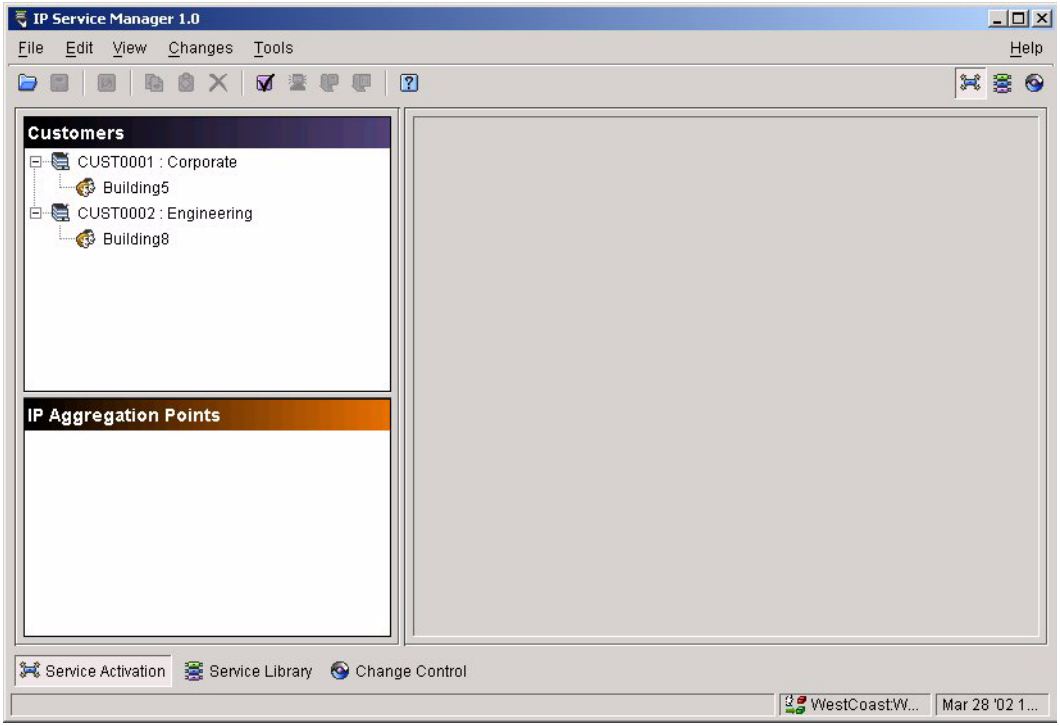


Figure 3-5: IPSM Service Activation View

The **Service Activation** view of IPSM allows you to manage subscribers, customers, and IP aggregation points. In IPSM, creating a subscriber creates a VLAN or sub-VLAN that contains one physical port on a network device. Service is provided to a subscriber

through that port. Customers consist of one or more subscribers. Creating an IP aggregation point creates a super-VLAN (used to contain a subscriber's sub-VLAN).

When you create a subscriber, you will also associate a a service bundle with that subscriber. A service bundle is a specific Qos profile and group of access lists.

Service Library View

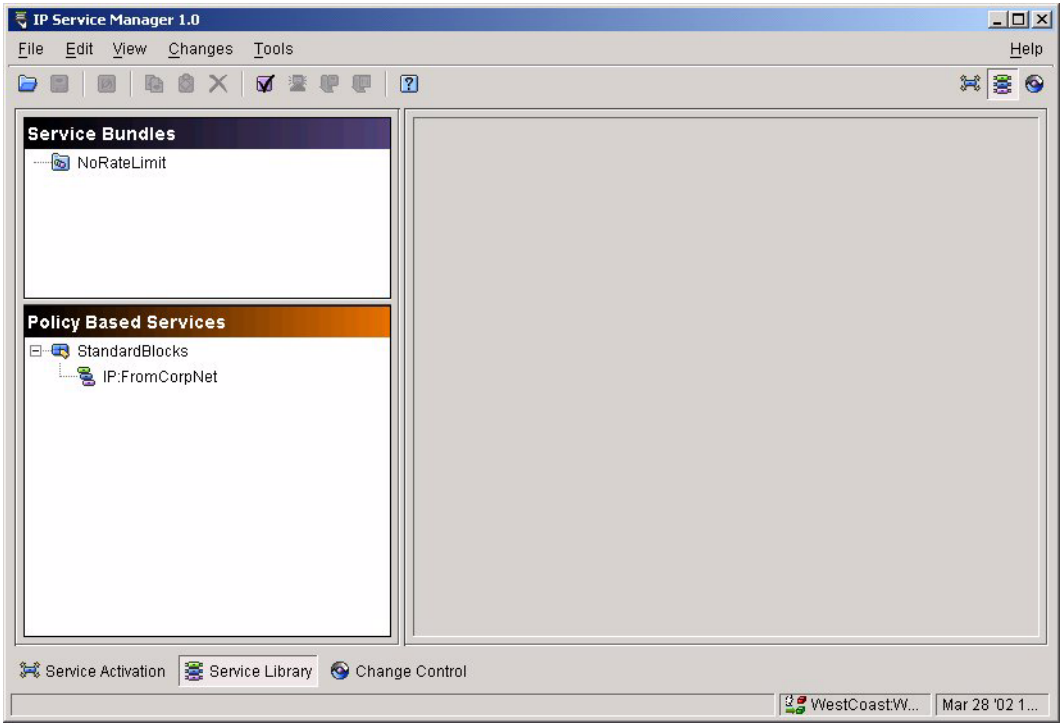


Figure 3-6: Service Library View

The **Service Library** view allows you to manage service bundles and policy based services (consisting of IP, TCP, and UDP traffic policies). Creating a service bundle in IPSM creates a QoS profile, and creating a policy based service creates an access list in the ISM Provision database. Once a service bundle is associated with a subscriber, the QoS profile and access lists are created on the device configurations in ISM Provision.

Change Control View

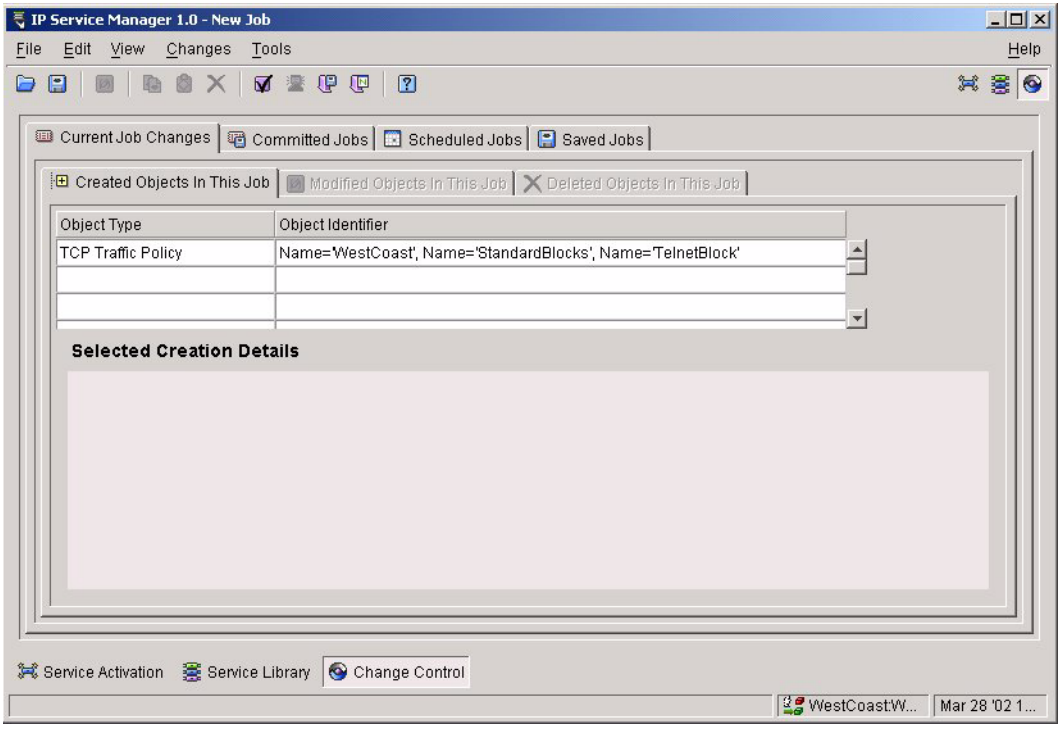


Figure 3-7: Change Control View

From the **Change Control** view you can manage the changes you create with IPSM. For your current session, you can see the changes that you have made and not yet saved or committed to the network. There is a record of changes committed to the network and changes scheduled to be committed to the network.

You can also review the changes that you have saved or committed from this view.

IPSM Icons

There are a number of icons visible from all of the IPSM views. When the function associated with an icon is available, the icon is in color. When the icon function is not available, the icon is greyed out.

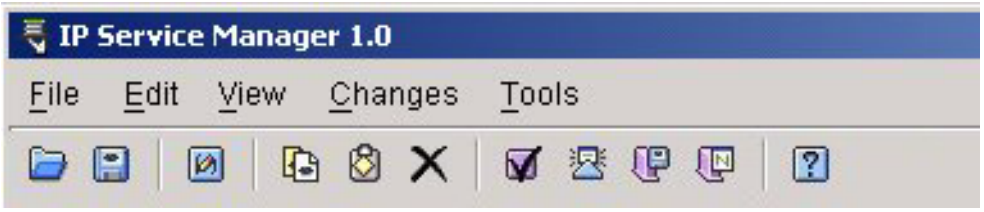


Figure 3-8: IPSM Icons: Open Changes, Save Changes, Modify Object, Copy, Paste, Delete, Verify Configuration, Synchronize, Commit Changes, Revert Changes, Help

Open Changes

Select this icon to open changes that you have previously saved to the ISM Provision server. The changes will be incorporated into your Network Provision view. Once opened, you can further modify the Network Provision view, or commit the changes to the network.

Save Changes

Select this icon to save changes that you have made. Saved changes are not pushed out to the network devices, but are saved on the ISM Provision server for further work, or to be viewed by others.

Modify Object

Select this icon to modify the currently selected object. In general, an object-specific wizard will open to allow you to change the object properties.

Copy

Select this icon to copy the currently selected object.

Paste

Select this icon to paste the previously copied object.

Delete

Select this icon to delete the currently selected object.

Verify Configuration

Select this icon to check your changes against the ISM Provision rules. If errors are found, they will be identified, and you can change them.

Synchronize

Select this icon to merge the changes from the server into your view, if you did not update your view when first notified.

When the network configuration changes because of the actions of another user, the ISM Provision server changes. Your current view is now out of sync with the server. The ISM Provision server notifies the IPSM client and displays the S**erver Update Notification** dialog box (if this option is set). From this box you can either select **Update Now** or **Update Later**. By selecting **Update Now**, the server changes are merged into your view. If you select **Update Later**, the **Synchronize** icon becomes available. At a later time you can then select the icon, and merge the sever changes into your view.

Commit Changes

Select this icon to commit your changes to ISM Provision. The changes are incorporated into the ISM Provision server and the device configurations are changed.

Revert Changes

Select this icon to discard changes you have made in IPSM. Your changes will be removed and your view will be refreshed from the server.

Help

Select this icon to open a browser and display this document.

4 Service Library

Overview

The **Service Library** view of IP Service Manager allows you to create and modify the services available to the subscribers you create in the **Service Activation** view. The services created in the **Service Library** view are associated with particular subscribers in the **Service Activation** view, which in turn creates changes in the device configurations in ISM Provision.

This chapter explains the following concepts about the **Service Library** view of IPSM:

- Traffic Policies
- Policy Based Services
- Service Bundles
- Service Categories
- Key Information

This chapter also explains how to perform a number of tasks in the **Service Library** view of IPSM. The following tasks are documented in this section:

- Add a Service Bundle
- Add a Policy Based Service
- Add an IP, TCP or UDP Traffic Policy

Traffic Policies

A traffic policy is similar to an access list in ExtremeWare. You can specify IP, TCP, and UDP traffic policies to specify the handling of various kinds of traffic. Just like an access list, you specify source, destination, and precedence for the traffic policies. Unlike access lists, there is no “deny” or “permit” parameter for traffic policies. The deny/permit functionality is implemented when you create policy based services. A traffic policy that is part of a policy based service configured to “block” traffic is equivalent to an access list set to “deny”. A traffic policy that is part of a policy based service configured to either “no rate limiting” or “use rate limiting” is equivalent to an access list set to “permit” (the rate limiting may cause the traffic to be dropped because of congestion, but that is different from an outright “deny”).

Policy Based Services

A policy based service consists of at least one traffic policy and a specification of the behavior for the service. A policy based service only applies to the ingress traffic of a subscriber. The ingress behavior can be set to “blocked”, “no rate limiting”, or “use rate limiting”. If the “use rate limiting” parameter is set, there must be a loopback port/VLAN defined for the subscriber that the policy based service is eventually applied to. Those policy based services set to “use rate limiting” will set one of the QoS profiles (Qp2 through Qp8) on the subscriber loopback VLAN. You cannot manually assign which service uses which profile.

Policy based services are not used directly by subscribers, but are part of service bundles. A single policy based service can belong to more than one service bundle.

Service Bundles

A service bundle can be thought of as the default behavior for a subscriber’s ingress and egress traffic, modified by any policy based services added to the service bundle. This service bundle will be associated with a subscriber (created in **Service Activation** view), to control the traffic on that subscriber’s port. If there are no policy based services added to the service bundle, the service bundle sets the behavior for all of the traffic for a subscriber.

The egress rate limiting behavior of a service bundle is applied to the default QoS profile (Qp1) on the subscriber port, and the ingress behavior is applied to Qp1 on the subscriber's loopback port.

Service Categories

The service categories specify the speed of the port to which the services will be applied. The supported categories are 10, 100, and 1000 Mbps. Changing the service category affects the rate limiting choices on the system. The service category of a policy based service must match the service category of the service bundle to which it is added, as well as the subscriber's port speed.

Key Information

A configuration object managed by ISM Provision is tracked by its object type and its key information. No other object of that type can use the same key information. When you create an object you supply its key information, denoted by a field that ends with an asterisk (*). For example, when you create a service bundle, you type the key information into the **Name*** field. No other service bundle can use this identifier. Since ISM Provision tracks an object by its key information, you cannot modify key information for objects. You can modify other parameters for objects, but not the key. If you want to have an object with the same parameters but different key information, you will need to copy the object, and provide the new key information when you paste it.

Service Library Tasks

The following tasks are performed in the Service Library view of IP Service Manager:

- Add a Service Bundle
- Add a Policy Based Service
- Add an IP, TCP or UDP Traffic Policy

Add a Service Bundle

When you add a service bundle, you will specify the default ingress and egress behavior, and add any policy based services. The service bundle that you create will then be available to apply to the subscribers that you created in the **Service Activation** view.

Summary Steps. To add a service bundle:

1 **Launch the Create Service Bundle wizard**

2 **Enter the service bundle name**

3 **Select the service category**

4 **Set the default ingress and egress behavior**

5 **Add policy based services**

6 **Select Finish**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a service bundle:

1 **Launch the Create Service Bundle wizard**

To launch the **Create Service Bundle** wizard, select **Edit>Add>Service Bundle** from the menu, or right-click in the **Service Bundles** panel and select **Add>Service Bundle** from the pop-up menu. The **Create Service Bundle** wizard will appear (see Figure 4-1).

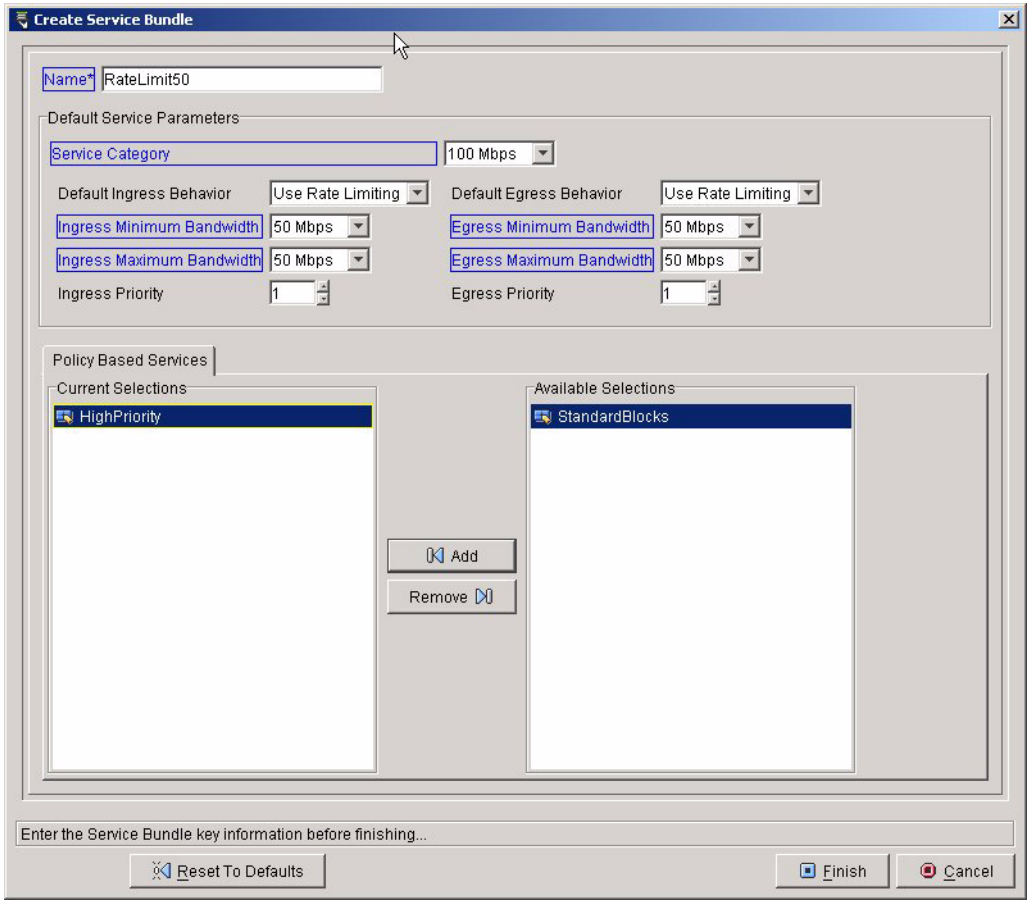


Figure 4-1: Create Service Bundle Wizard

2 Enter the service bundle name

The name is the key information for the service bundle. Once you have entered the key information you can close the wizard by selecting **Finish**, but you still may need to configure other parameters before you have a valid configuration. Figure 4-2 shows the upper part of the **Create Service Bundle** wizard in more detail.

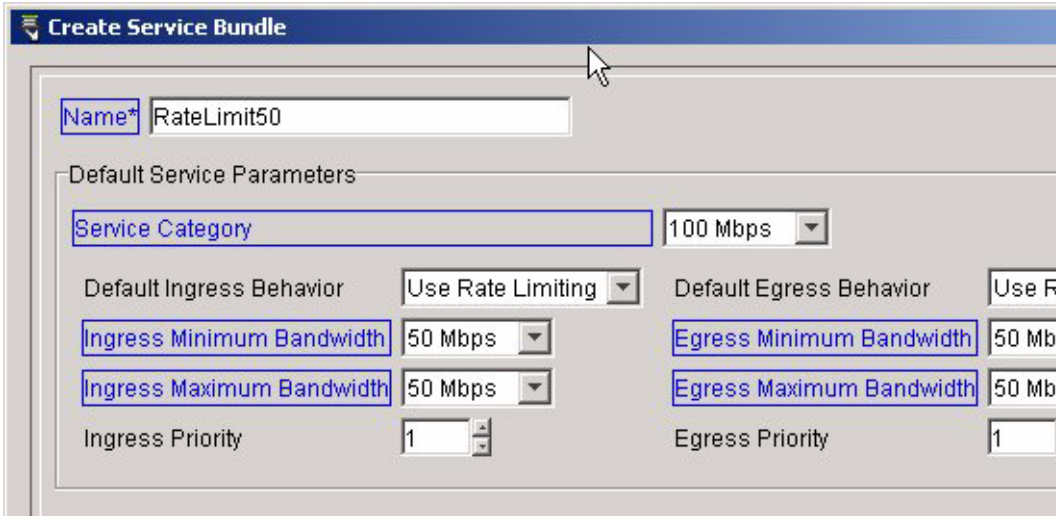


Figure 4-2: Create Service Bundle Upper Detail

3 Select the service category

Choose the service category based on the physical bandwidth of the port you will be applying this service to. Your choices are 10, 100, and 1000 Mbps.

4 Set the default ingress and egress behavior

Set the behavior to one of the selections in the drop-down list. If you choose "blocked" or "no rate limiting" the other choices are greyed out. If you choose "use rate limiting" then also select the minimum and maximum bandwidth and priority. For ingress rate limiting, the subscriber that you apply this service to must have a loopback port defined.

5 Add policy based services

Select the policy based services that you wish to add from the **Available Selections** panel by clicking on them, then select the **Add** button to move your selection to the **Current Selections** panel. These policy based services will now be part of the service bundle you are creating.

6 Select Finish

Select **Finish** to close the wizard.

Add a Policy Based Service

When you create a policy based service, you will specify whether traffic is blocked, will use no rate limiting, or will use rate limiting, and you will apply one or more traffic policies to the policy based service.

Summary Steps. To add a policy based service:

1. **Launch the Create Policy Based Service wizard**
2. **Enter the service name**
3. **Select the service category**
4. **Select the default ingress behavior**
5. **Add at least one traffic policy**
6. **Select Finish**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a policy based service:

1. **Launch the Create Policy Based Service wizard**

   To launch the **Create Policy Based Service** wizard, select **Edit>Add>Policy Based Service** from the menu, or right-click in the **Policy Based Service Bundles** panel and select **Add>Policy Based Service** from the pop-up menu. The **Create Policy Based Service** wizard will appear (see Figure 4-3).

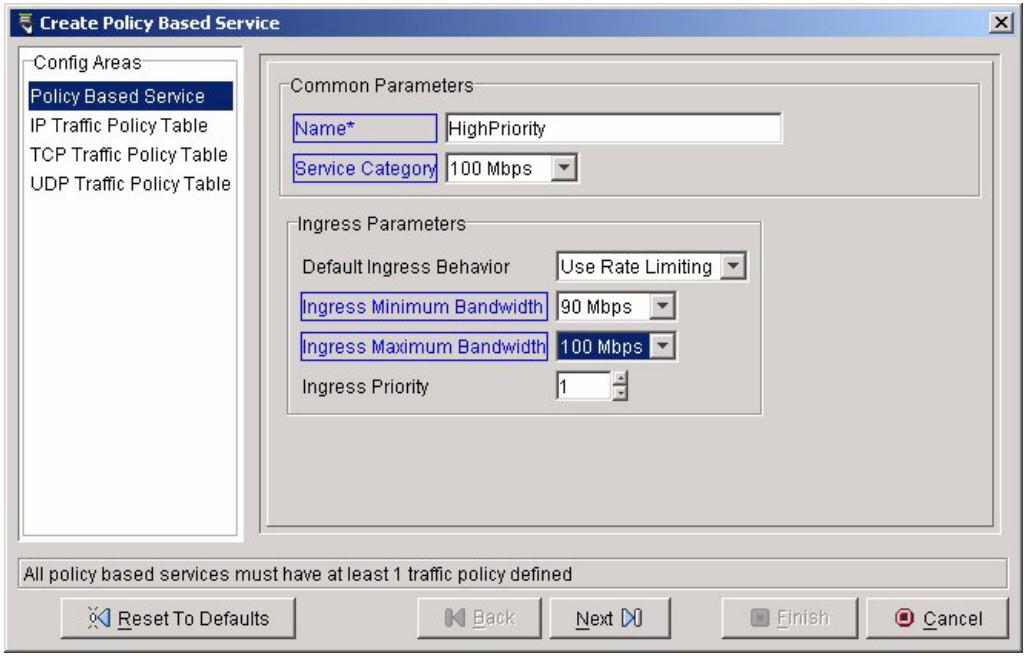


Figure 4-3: Create Policy Based Service Wizard

2 Enter the service name

The name is the key information for the policy based service, but you must also add at least one traffic policy before you can create a policy based service.

3 Select the service category

Choose the service category based on the physical bandwidth of the port you will be applying this service to. Your choices are 10, 100, and 1000 Mbps. The service category of a policy based service must match the service category of any service bundles that it will be applied to.

4 Select the default ingress behavior

Set the behavior to one of the selections in the drop-down list. If you choose "blocked" or "no rate limiting" the other choices are greyed out. If you choose "use rate limiting" then also select the minimum and maximum bandwidth and priority. For ingress rate limiting, the subscriber that you apply this service to must have a loopback port defined.

5 Add at least one traffic policy

Select one of the entries in the **Config Areas** panel, or select **Next** to go to one of the **Traffic Policy Table** pages. From here, select the plus sign (+) icon to launch the **Create IP**, **TCP**, or **UDP Traffic Policy** wizard (see Figure 4-4).

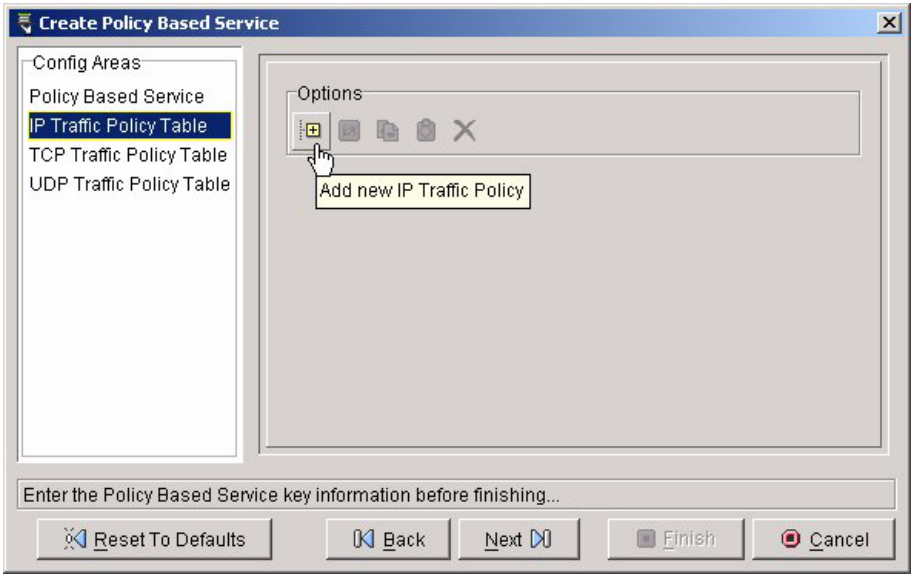


Figure 4-4: Launching the Create IP Traffic Policy Wizard

See the task section, “Add an IP, TCP or UDP Traffic Policy”, for details on adding a traffic policy once you’ve launched the wizard. Once you’ve added a traffic policy, you can select **Finish**, or you can add other traffic policies by selecting the desired page and clicking the plus sign (+) icon again.

6 Select Finish

Select **Finish** to close the wizard.

Add an IP, TCP or UDP Traffic Policy

The steps to create traffic policies are identical for IP, TCP, and UDP, except that you do not specify source and destination ports for IP traffic policies. In the following task any reference to “traffic policy” includes all three types, unless specifically called out. So a reference to the **Create Traffic Policy** wizard includes the **Create IP Traffic Policy**, **Create TCP Traffic Policy**, and **Create UDP Traffic Policy** wizards.

Summary Steps. To add a traffic policy:

1 Launch the Create Traffic Policy wizard

2 Enter the policy name

3 Enter the source and destination subnets

4 Enter the policy precedence

5 For TCP and UDP, enter the source and destination ports

6 Select Finish

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a traffic policy:

1 Launch the Create Traffic Policy wizard

To launch the **Create Traffic Policy** wizard, select **Edit>Add>Traffic Policy** from the menu, or right-click a policy based services entry in the **Policy Based Services** panel and select **Add>Traffic Policy** from the pop-up menu. The **Create Traffic Policy** wizard will appear. Figure 4-5 shows the **Create TCP Traffic Policy** wizard. The UDP wizard looks almost identical, and the IP wizard does not have the port specification fields.

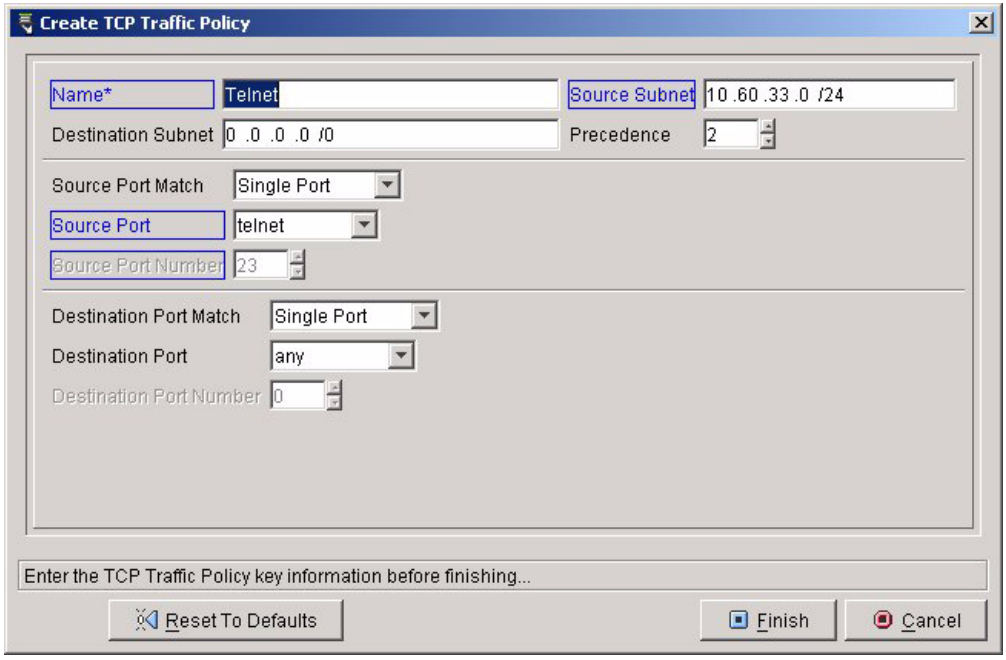


Figure 4-5: Create TCP Traffic Policy Wizard.

2 Enter the policy name

The name is the key information for the traffic policy. Once you have entered the key information you can close the wizard by selecting **Finish**, but you still may need to configure other parameters before you have a valid configuration.

3 Enter the source and destination subnets

Specify the source and destination subnets of the traffic you will apply the traffic policies to.

Traffic policies are applied to the ingress traffic on the subscriber port.

4 Enter the policy precedence

Like access lists, traffic policies have a precedence associated with them. The traffic policies are applied in precedence order, as are access lists. Precedence numbers must be unique among all the traffic policies applied to a particular subscriber.

5 For TCP and UDP, enter the source and destination ports

For the **Source Port Match** field, choose **Single Port** or **Range Of Port**s from the drop-down list.

If you choose **Single Port**, choose the **Source Port** from the drop-down list. Your **Source Port** choices are **any**, **user defined**, or a list of well known services like **telnet**, **finger** or **tftp**. If you choose **user defined**, you will also choose the **Source Port Number**, otherwise the port number will be filled in for the well known services, or left blank for **any** port (see Figure 4-6).

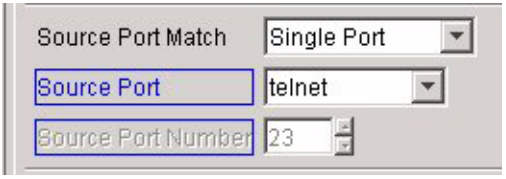


Figure 4-6: Specifying a Single Port in a Traffic Policy

If you choose **Range Of Ports**, the wizard will change so you can specify the **Start Source Port Number** and the **End Source Port Number** (see Figure 4-7).

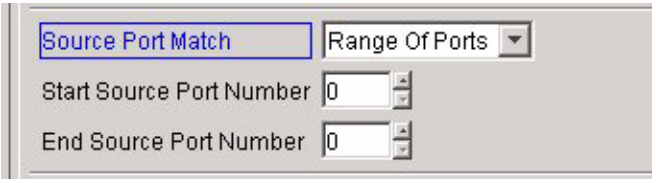


Figure 4-7: Specifying a Range of Ports in a Traffic Policy

6 Select Finish

Select **Finish** to close the wizard.

5 Service Activation

Overview

The **Service Activation** view of IP Service Manager allows you to control the services provided to your network subscribers. A subscriber in IPSM represents a VLAN that contains one port, so when you create a subscriber in IPSM, a VLAN is added to the device configuration. A customer is a group of subscribers.

The chapter explains the following concepts about the **Service Activation** view:

- Subscriber
- Customer
- IP Aggregation Point

This chapter also explains how to perform a number of tasks in the **Service Activation** view:

- Add a Customer
- Add an IP Subscriber
- Add an IP Range Subscriber
- Add an IP Aggregation Point

Subscriber

A subscriber is a port and a VLAN that provides access to the network for specified traffic with a specified Quality of Service (QoS). When you create a subscriber in IP Service Manager, the ISM Provision server makes changes to the device configurations to create the VLAN, Qos profiles, and access lists implied by your subscriber. There are two types of subscribers, IP subscribers and IP range subscribers.

IP subscribers correspond to a port and a VLAN with an assigned IP subnet for routing purposes. The service provided through this port can support hosts configured with IP addresses that lie in the VLAN's subnet.

IP range subscribers correspond to a port and a sub-VLAN. This sub-VLAN is associated with a super-VLAN and its IP subnet (in IP Service Manager a super-VLAN is called an IP aggregation point). The IP range subscriber is assigned IP numbers from this subnet. The service provided through this port can support hosts configured with the IP numbers in this range.

Customer

A customer is a collection of subscribers. Since a subscriber can only apply to one port, anytime that you need to provide more than one port of service to an organization, you will organize the individual ports as subscribers, and the whole organization as the customer.

IP Aggregation Point

An IP aggregation point is a super-VLAN to which the IP range subscribers are associated. Each IP range subscriber is on its own sub-VLAN associated with the IP aggregation point, a super-VLAN.

Service Activation Tasks

The following tasks are performed in the **Service Activation** view of IP Service Manager:

- Add a Customer
- Add an IP Subscriber
- Add an IP Range Subscriber
- Add an IP Aggregation Point

Add a Customer

A customer is a way to organize a collection of subscribers. A customer might be an actual external customer, an internal customer like a department that is billed for services, or a fictional “customer” for the purposes of naming and organizing subscribers. When you create a customer, you also have the option of creating subscribers at the same time, or creating them later.

Summary Steps. To add a customer:

1 Launch the Create Customer wizard

2 Enter the Customer ID

3 Enter the Customer Name

4 Select Next and add subscribers

5 Select Finish

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a customer:

1 Launch the Create Customer wizard

To launch the Create Customer wizard, you can either select the **Edit>Add>Customer** menu item, or right-click the mouse in the **Customers** panel of the **Service Activation** view and select **Add>Customer** from the pop-up menu (see Figure 5-1).

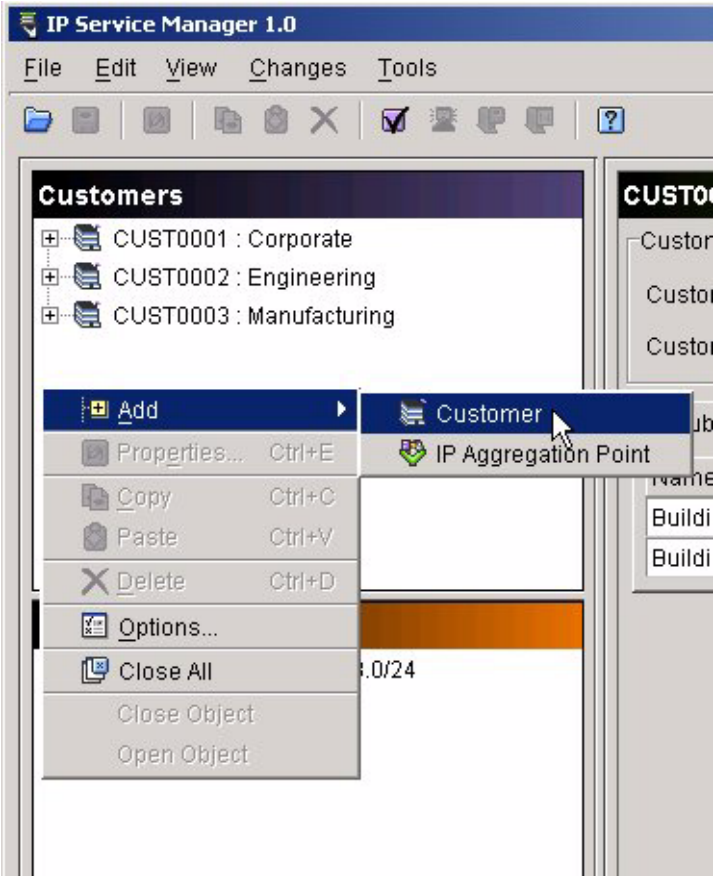


Figure 5-1: Launching the Create Customer Wizard

2 Enter the Customer ID

Once the **Create Customer** wizard has appeared, enter the **Customer ID**. You must enter this key information in order to create the customer. All the other information is optional, however, you will eventually need to define either an IP subscriber or an IP range subscriber (see Figure 5-2).

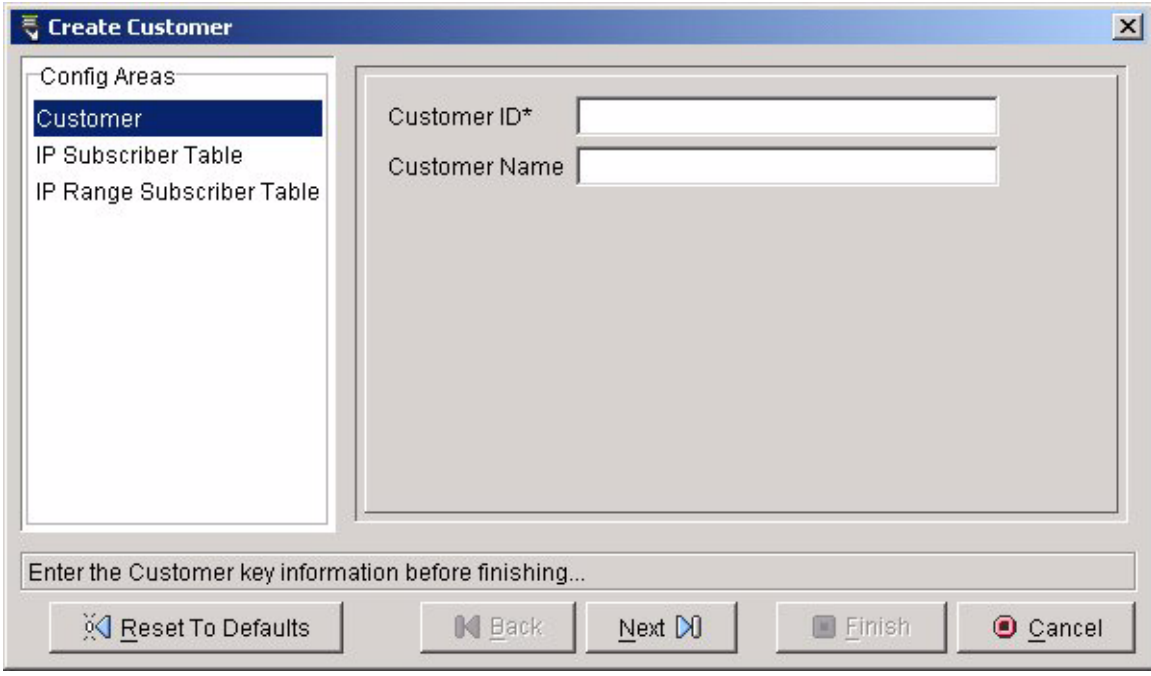


Figure 5-2: Create Customer Wizard

3 Enter the Customer Name

Enter the name you wish to use to describe the customer in the **Customer Name** field.

4 Select Next and add subscribers

To add subscribers, select **Next** to move to the next **Config Areas** page. Add IP subscribers on the **IP Subscriber Table** page and IP range subscribers on the **IP Range Subscriber Table** page. Click the plus sign (+) to launch the **Create IP Subscriber** or **Create IP Range Subscriber** wizard (see Figure 5-3).

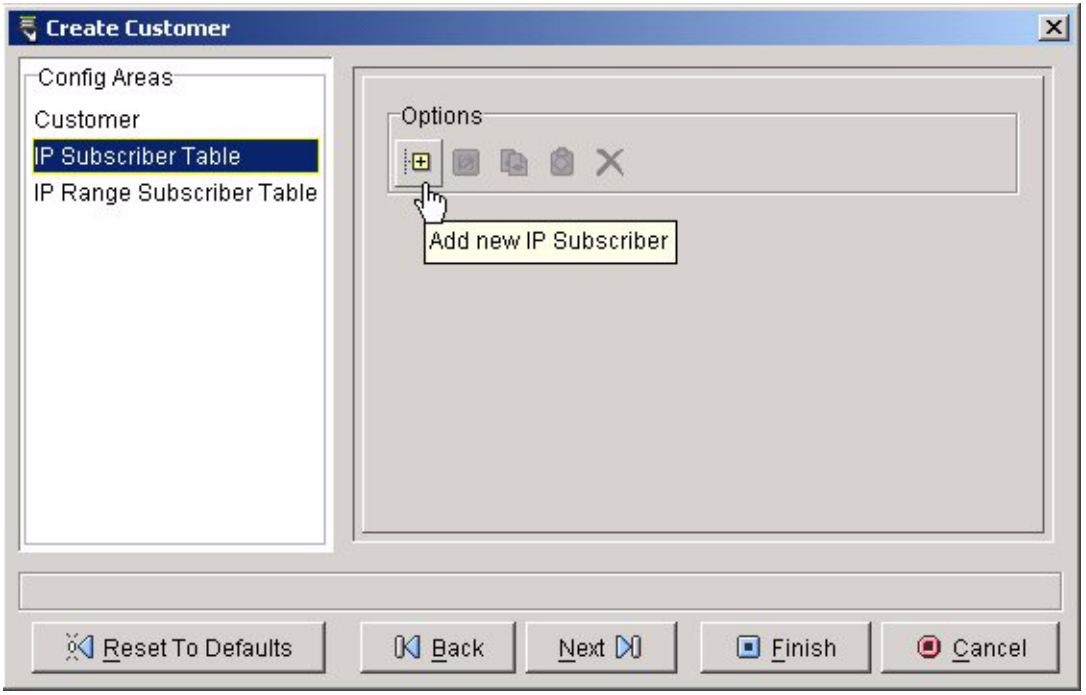


Figure 5-3: IP Subscriber Table in the Create Customer Wizard

Once the wizard launches, add the information for the subscriber (see Figure 5-4). For more information about the **Create IP Subscriber** and **Create IP Range Subscriber** wizards and adding IP subscribers, see the tasks, “Add an IP Subscriber”, and “Add an IP Range Subscriber”. Once you’ve added the subscriber, select **Finish** to close the subscriber wizard. You can repeat the process to add more subscribers to the customer, or go to the next step, closing the **Create Customer** wizard.

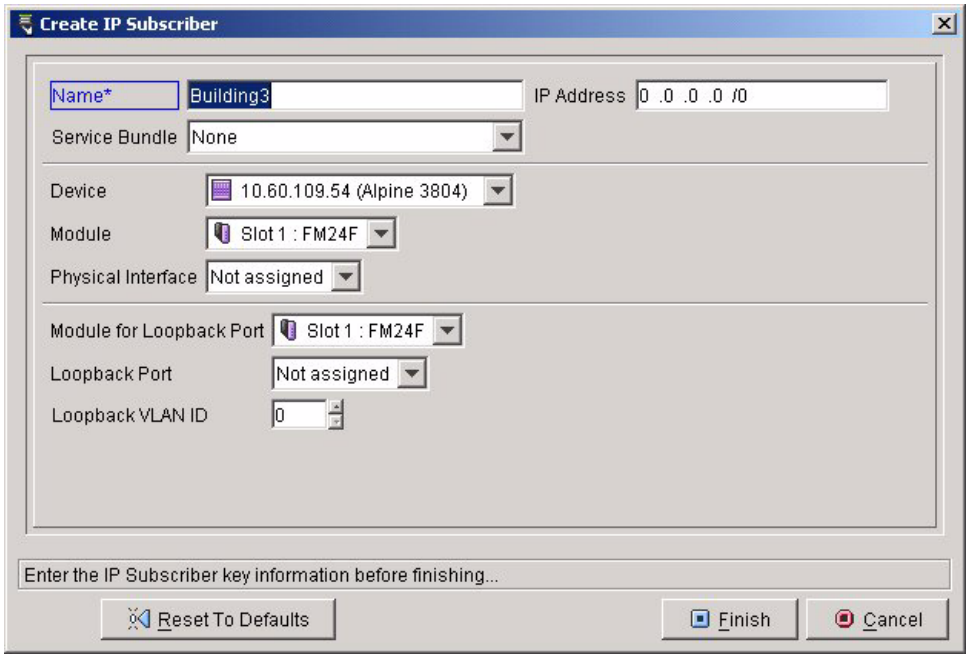


Figure 5-4: Create IP Subscriber W)izard

5 Select Finish

Select **Finish** to close the **Create Customer** wizard.

Add an IP Subscriber

When you create an IP subscriber, you are defining a single port VLAN on a device, and that single port will be providing network services to any devices connected through that port. You will essentially be creating a VLAN / IP subnet to deliver service.

For more information about how the IP subscriber parameters affect the operation of the created VLAN on the device, see the *ExtremeWare Software User Guide.*

Summary Steps. To add an IP subscriber:

1 Launch the Create IP Subscriber wizard

2 Enter the subscriber name

3 Enter the IP address and subnet mask

4 Choose a service bundle

5 Choose a device, module, and physical interface

6 Choose a loopback module, port, and VLAN ID

7 Select Finish to close the wizard

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add an IP subscriber:

1 Launch the Create IP Subscriber wizard

To launch the **Create IP Subscriber** wizard, select **Edit>Add>IP Subscriber** from the menu, or right-click a customer entry in the **Customers** panel and select **Add>IP Subscriber** from the pop-up menu. The **Create IP Subscriber** wizard will appear (see Figure 5-5).

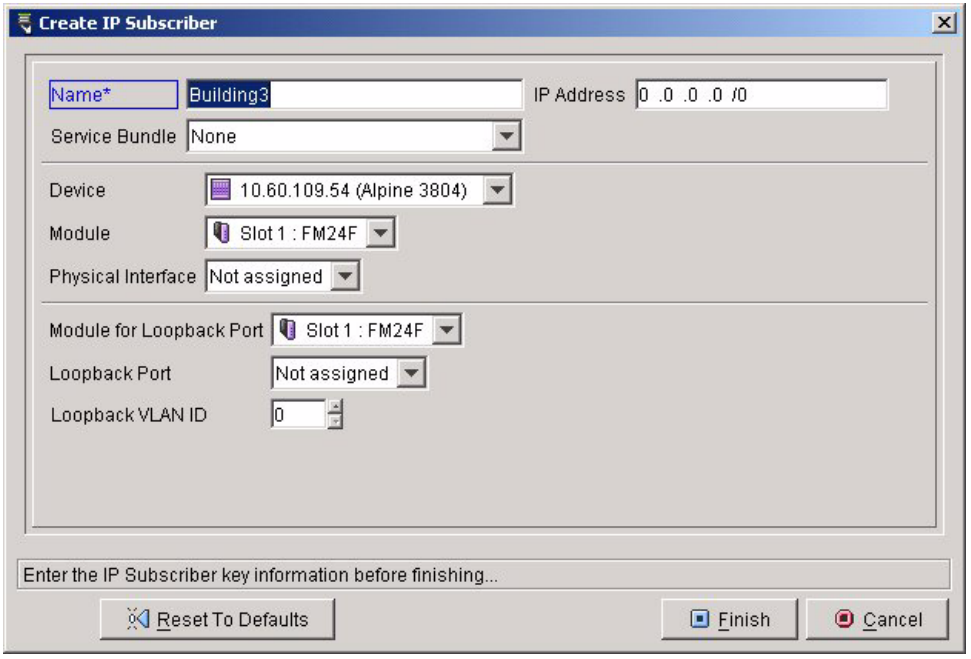


Figure 5-5: Create IP Subscriber Wizard

2 Enter the subscriber name

The subscriber name is the key information for the subscriber. Once you have entered the key information you can close the wizard by selecting **Finish**, but you still may need to configure other parameters before you have a valid configuration. For example, you may want to create a subscriber, and then go on to specify a service bundle in the **Service Library** view, returning later to associate the service bundle with the subscriber.

3 Enter the IP address and subnet mask

Any host IP addresses on this subscriber port must fall within the subnet that you specify.

4 Choose a service bundle

Use the drop-down list **Service Bundle** to select the service bundle for this subscriber. Service bundles are defined in the **Service Library** view of IPSM. See Chapter 4, “Service Library”, for more information. If you do not choose a service bundle, there will be no access lists, or rate limiting QoS profiles associated with this subscriber.

You can add a service bundle or change the service bundle at a later time.

5 Choose a device, module, and physical interface

Use the drop-down lists to choose a device, module (slot), and port for the subscriber. For devices that do not have multiple modules, the module list defaults to the entry, **Ports**, and you select the port from the **Physical Interface** list.

6 Choose a loopback module, port, and VLAN ID

If the subscriber requires ingress rate-shaping, you will need to specify all of the above information.

7 Select Finish to close the wizard

Add an IP Range Subscriber

When you create an IP range subscriber, you are defining a single port sub-VLAN on a device, and that single port will be providing network services to any devices connected through that port. Sub-VLANs in ExtremeWare are associated with a super-VLAN, so IP range subscribers in IPSM are associated with IP aggregation points. You will eventually need to associate any IP range subscriber that you create with an IP aggregation point.

For more information about how the IP range subscriber parameters affect the operation of the created sub-VLAN on the device, and for more information on sub-VLANs,

super-VLANs in general, and VLAN aggregation, see the *ExtremeWare Software User Guide.*

Summary Steps. To add an IP range subscriber:

1. **Launch the Create IP Range Subscriber wizard**
2. **Enter the subscriber name**
3. **Enter the VLAN tag**
4. **Select the IP aggregation point**
5. **Enter the IP range start and range end**
6. **Select a service bundle**
7. **Choose a device, module, and physical interface**
8. **Choose a loopback module, port, and VLAN ID**
9. **Select Finish to close the wizard**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add an IP range subscriber

1 Launch the Create IP Range Subscriber wizard

To launch the **Create IP Range Subscriber** wizard, select **Edit>Add>IP Subscriber** from the menu, or right-click a customer entry in the **Customers** panel and select **Add>IP Subscriber** from the pop-up menu. The **Create IP Range Subscriber** wizard will appear (see Figure 5-6).

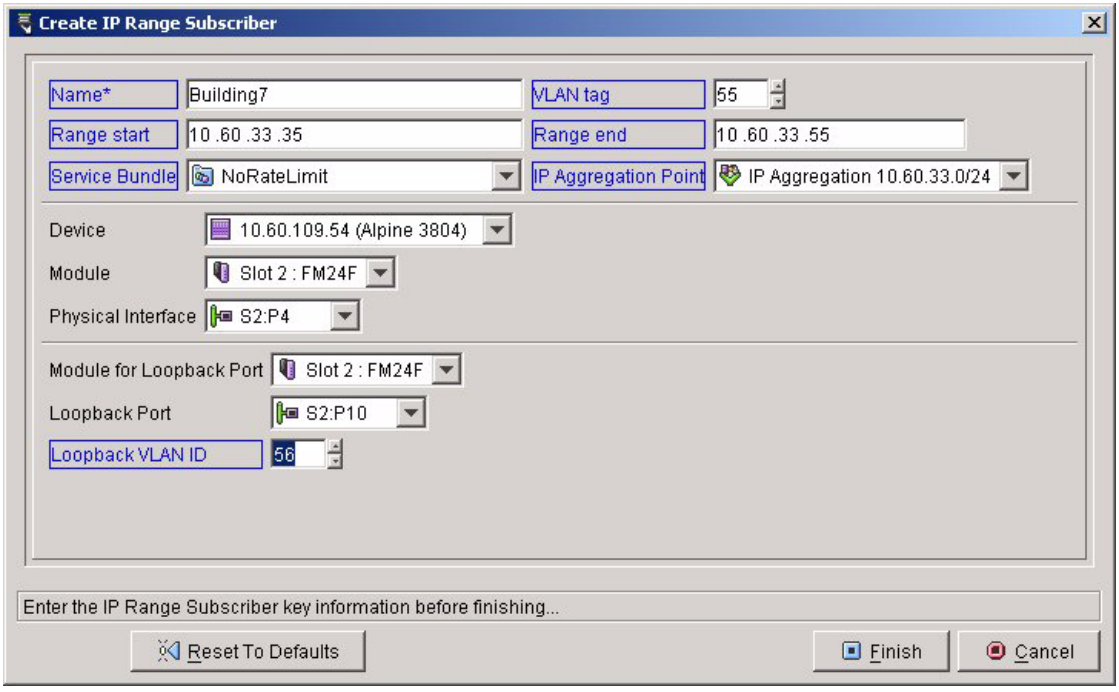


Figure 5-6: Create IP Range Subscriber Wizard

2 Enter the subscriber name

The subscriber name is the key information for the subscriber. Once you have entered the key information you can close the wizard by selecting **Finish**, but you still may need to configure other parameters before you have a valid configuration. For example, you may want to create a subscriber, and then go on to specify a service bundle in the **Service Library** view, returning later to associate the service bundle with the subscriber.

3 Enter the VLAN tag

Enter the VLAN tag to use if the IP range subscriber and IP aggregation point are on different devices.

4 Select the IP aggregation point

The IP aggregation point represents the super-VLAN that this IP range subscriber sub-VLAN is associated with. Every IP range subscriber must eventually be associated with an IP aggregation point. The IP aggregation point can be on the same device as the IP range subscriber or it will be automatically setup if it is one

layer 2 hop away (and the trunk connection is defined in Network Infrastructure Manager).

5 Enter the IP range start and range end

These parameters specify the IP addresses allowed for this IP range subscriber. Any The addresses must be contained in the subnet specified for the IP aggregation point.

6 Select a service bundle

Use the drop-down list **Service Bundle** to select the service bundle for this subscriber. Service bundles are defined in the **Service Library** view of IPSM. See Chapter 4, “Service Library”, for more information. If you do not choose a service bundle, there will be no access lists, QoS profiles, or rate limiting associated with this subscriber.

You can add a service bundle or change the service bundle at a later time.

7 Choose a device, module, and physical interface

Use the drop-down lists to choose a device, module (slot), and port for the subscriber. For devices that do not have multiple modules, the module list defaults to the entry, **Ports**, and you select the port from the **Physical Interface** list.

8 Choose a loopback module, port, and VLAN ID

If the subscriber requires ingress rate-shaping, you will need to specify all of the above information.

9 Select Finish to close the wizard

Add an IP Aggregation Point

An IP aggregation point in IP Service Manager corresponds to a super-VLAN (the VLAN aggregation feature) in ExtremeWare. When you create an IP range subscriber in IPSM (which corresponds to a sub-VLAN in ExtremeWare), you must also eventually associate an IP aggregation point with that subscriber. To specify the IP aggregation point, you will specify an IP network address and netmask, and a device. A super-VLAN will be created on that device.

Summary Steps. To create an IP aggregation point:

1 Launch the Create IP Aggregation Point wizard

2 Enter the IP network address and netmask

3 Select the device

4 Select Finish to close the wizard

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To create an IP aggregation point:

1 Launch the Create IP Aggregation Point wizard

To launch the **Create IP Range Subscriber** wizard, select **Edit>Add>IP Aggregation Point** from the menu, or right-click in the **IP Aggregation Point** panel and select **Add>IP Aggregation Point** from the pop-up menu. The **Create IP Aggregation Point** wizard will appear

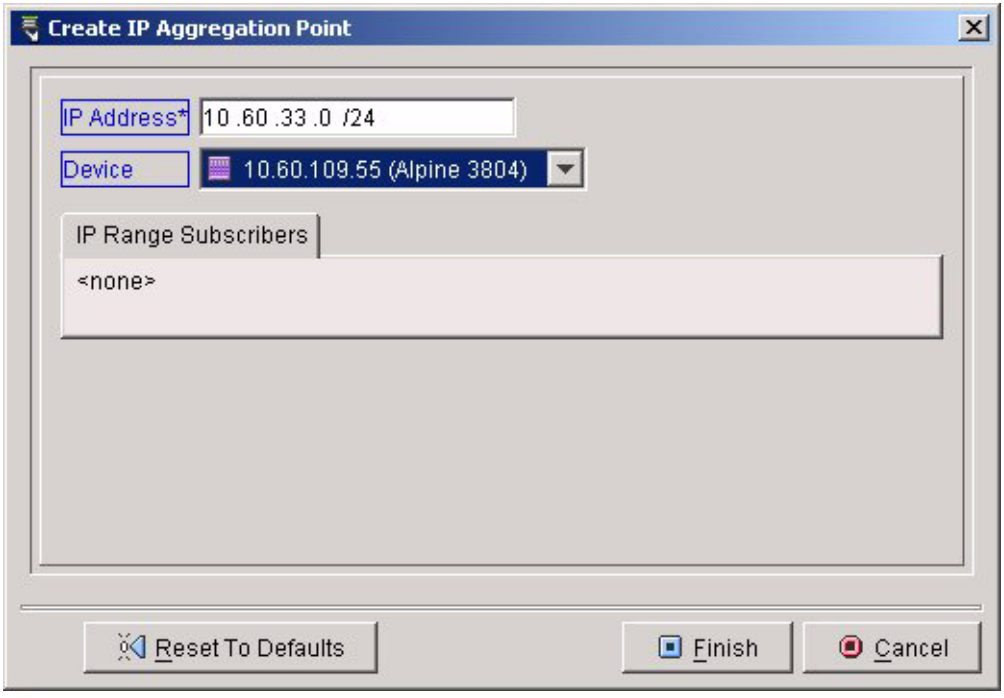


Figure 5-7: Create IP Aggregation Point Wizard

2 Enter the IP network address and netmask

This is the key information for the IP aggregation point. If device access has been defined in Network Infrastructure Manager, then the IP aggregation point IP address must come from the allowable pool of addresses.

3 Select the device

IPSM will create the IP aggregation point's super-VLAN on this device.

4 Select Finish to close the wizard

The **IP Range Subscribers** tab initially displays no entries. You can add the subscribers later, either when they are created, or you can modify the IP range subscribers to use this IP aggregation point. You cannot modify any of the IP aggregation point parameters once it is created.

6 Change Control

Overview

The **Change Control** view of IP Service Manager allows you to commit changes to the ISM Provision server, view the current uncommitted changes that you have made, and to view previously committed, scheduled, or saved changes.

This chapter explains the following concepts about the **Change Control** view of IPSM:

- Jobs

This chapter explains the following tasks that can be accomplished in the **Change Control** view of Network Infrastructure Manager:

- View Current Job Changes
- View Committed, Scheduled, or Saved Jobs
- Delete Scheduled or Saved Jobs

Jobs

Every time you add, modify, or delete any object, this change is captured by the client to either save or commit to the ISM Provision server. When you save or commit your changes, this list of individual additions, modifications, and deletions is sent to the ISM Provision server as a single entity called a job. A job may consist of a single change to one device parameter or the addition of hundreds of configuration objects, but it is

saved or committed as a unit to the ISM Provision server. Once a job is committed, any changes to the configurations of managed devices are sent to the devices using the device communicator assigned to that device.

Different from a committed job is a saved job. A saved job is also stored in the ISM Provision server, but its collection of changes are not sent out to the network, unless the saved job is later committed. A scheduled job is a saved job that will automatically be committed at a scheduled time. One of the options of the commit process is to do the actual commit at a later time. Any job scheduled to be committed at a later time is saved until the commit time, and then committed to the network.

If an error occurs while a job is being committed, and any of the changes that make up the job cannot be committed, the entire job is rejected, and any parts of the job already added are backed out. A committed job that causes an error is still listed along with other committed jobs, but its status is listed as rejected. To correct the errors, view the committed yet rejected job, and review the job results. You will see the details of the problem that caused the error.

Any job can be viewed, whether committed, rejected, scheduled or saved. You can review the individual objects that were created, modified, and deleted. You can also review the results of the job to help you correct any errors that might have occurred.

Change Control Tasks

The following tasks can be accomplished in the **Change Control** view of Network Infrastructure Manager:

- View Current Job Changes
- View Committed, Scheduled, or Saved Jobs
- Delete Scheduled or Saved Jobs

View Current Job Changes

Every change you make in IP Service Manager is captured in the current job. If you want to see what changes have been made that are not yet committed to the ISM Provision server, you would view the current job changes. You will view the changes in the **Current Job Changes** tab of the **Change Control** view of IPSM.

Steps. To view the current job changes:

1 Select the Current Job Changes tab in Change Control view

2 Select the Created, Modified, or Deleted Objects In This Job tab

The three tabs on the **Current Job Changes** tab are: **Created Objects In This Job**, **Modified Objects In This Job**, and **Deleted Objects In This Job**. Each tab displays the object changes that are not yet committed to the ISM Provision server. Choose the category of changes you wish to view.

3 Select individual objects to view details (if any)

For some objects, more details are listed in the **Selected Details** panel. Click on the object, and selected details are displayed in the panel (see Figure 6-1).

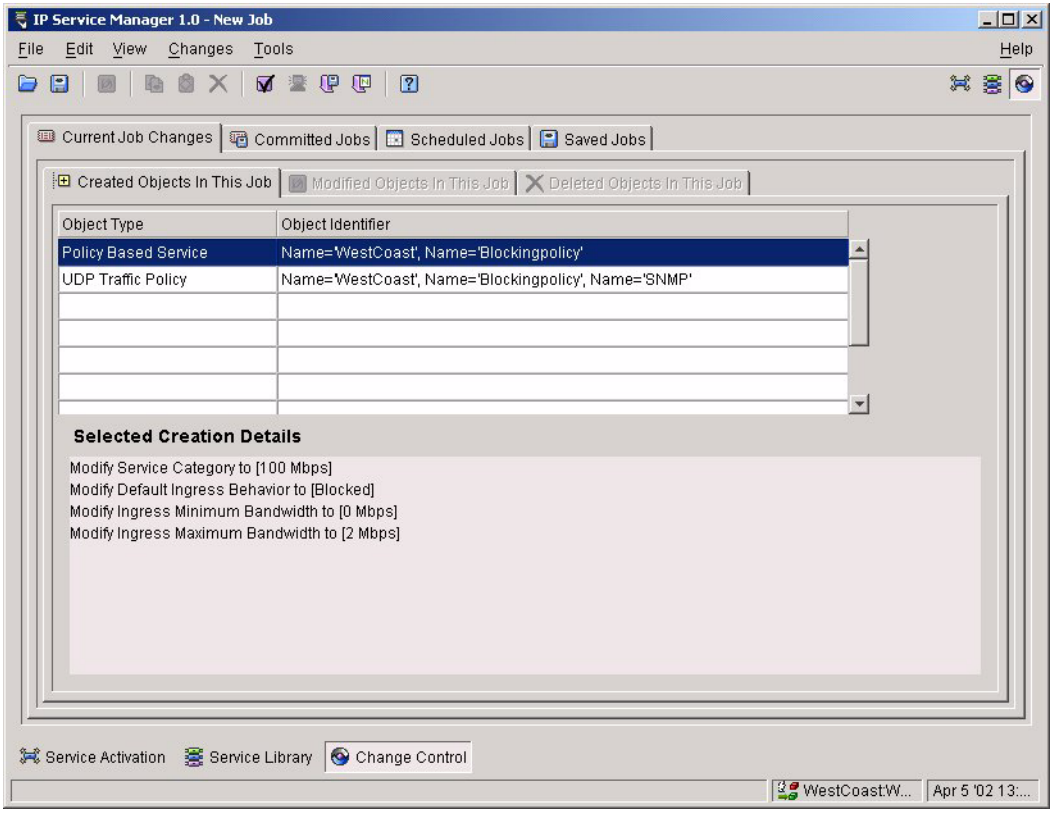


Figure 6-1: Current Job Changes

View Committed, Scheduled, or Saved Jobs

Committed, scheduled, and saved jobs are displayed on tabs in the **Change Control** view of IPSM. Once selected, you can review the job, and view the result of committing or saving it.

Summary Steps. To view a committed, scheduled, or saved job:

1 **Select the Committed, Scheduled, or Saved Jobs tab in the Change Control view**

2 **Select the job to review by clicking on the job name**

3 **Select the Review button**

4 **Review the job**

5 **Select Close**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To view a committed, scheduled, or saved job:

1 **Select the Committed, Scheduled, or Saved Jobs tab in the Change Control view**

From the Change Control view, select the tab for the job you want to view (see Figure 6-2).

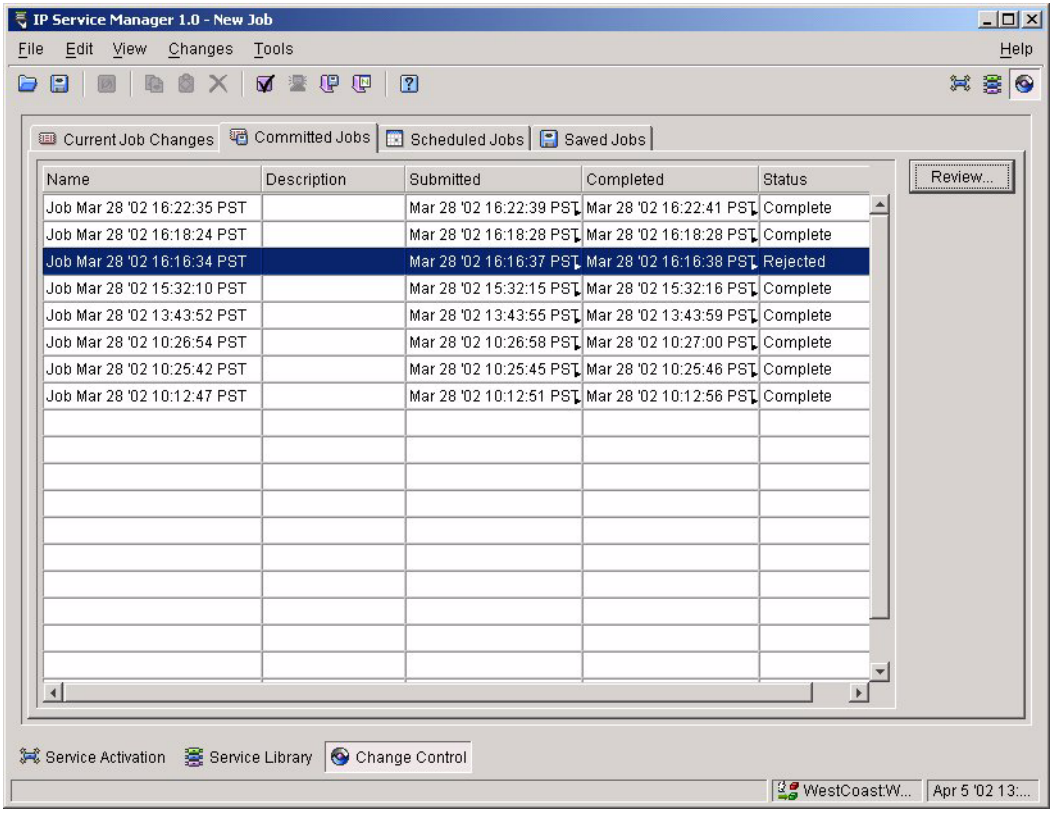

IP Service Manager 1.0 - New Job
File Edit View Changes Tools Help
Current Job Changes
Committed Jobs
Scheduled Jobs
Saved Jobs
Review...
Name | Description | Submitted | Completed | Status
Job Mar 28 '02 16:22:35 PST | | Mar 28 '02 16:22:39 PST | Mar 28 '02 16:22:41 PST | Complete
Job Mar 28 '02 16:18:24 PST | | Mar 28 '02 16:18:28 PST | Mar 28 '02 16:18:28 PST | Complete
Job Mar 28 '02 16:16:34 PST | | Mar 28 '02 16:16:37 PST | Mar 28 '02 16:16:38 PST | Rejected
Job Mar 28 '02 15:32:10 PST | | Mar 28 '02 15:32:15 PST | Mar 28 '02 15:32:16 PST | Complete
Job Mar 28 '02 13:43:52 PST | | Mar 28 '02 13:43:55 PST | Mar 28 '02 13:43:59 PST | Complete
Job Mar 28 '02 10:26:54 PST | | Mar 28 '02 10:26:58 PST | Mar 28 '02 10:27:00 PST | Complete
Job Mar 28 '02 10:25:42 PST | | Mar 28 '02 10:25:45 PST | Mar 28 '02 10:25:46 PST | Complete
Job Mar 28 '02 10:12:47 PST | | Mar 28 '02 10:12:51 PST | Mar 28 '02 10:12:56 PST | Complete
Service Activation
Service Library
Change Control
WestCoast:W...
Apr 5 '02 13:...

Figure 6-2: Committed Jobs Tab

2 Select the job to review by clicking on the job name

3 Select the Review button

Once you select the **Review** button, the **Details For Job** window opens.

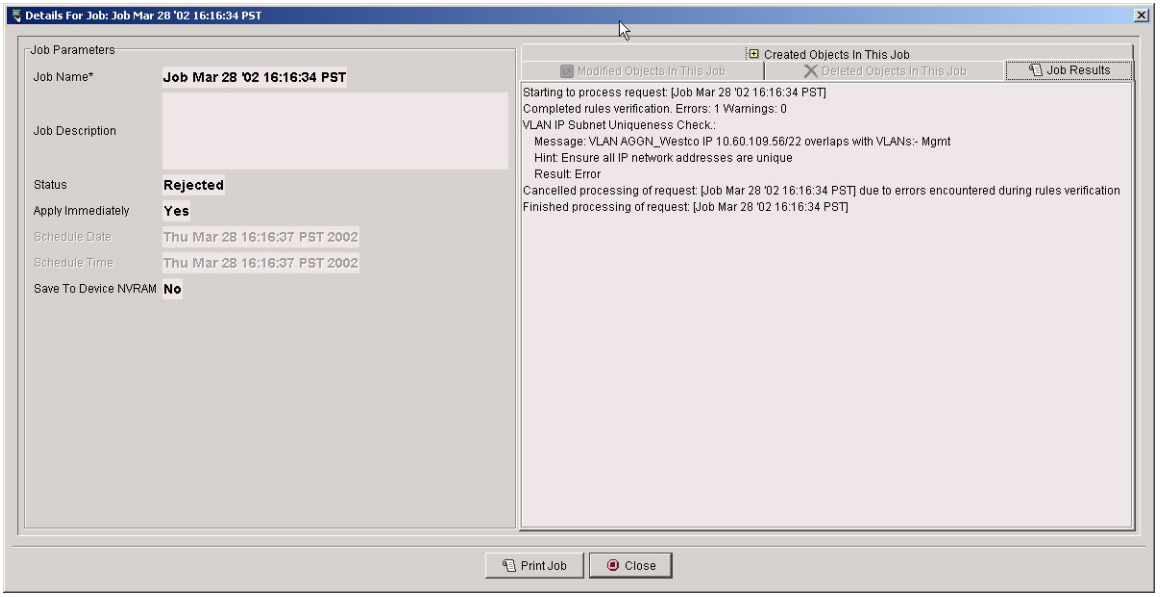

Details For Job: Job Mar 28 '02 16:16:34 PST
Job Parameters
Job Name*
Job Mar 28 '02 16:16:34 PST
Job Description
Status
Rejected
Apply Immediately
Yes
Schedule Date
Thu Mar 28 16:16:37 PST 2002
Schedule Time
Thu Mar 28 16:16:37 PST 2002
Save To Device NVRAM
No
Created Objects In This Job
Modified Objects In This Job
Deleted Objects In This Job
Job Results
Starting to process request: [Job Mar 28 '02 16:16:34 PST]
Completed rules verification. Errors: 1 Warnings: 0
VLAN IP Subnet Uniqueness Check.:
Message: VLAN AGGN_Westco IP 10.60.109.56/22 overlaps with VLANs:- Mgmt
Hint: Ensure all IP network addresses are unique
Result: Error
Cancelled processing of request: [Job Mar 28 '02 16:16:34 PST] due to errors encountered during rules verification
Finished processing of request: [Job Mar 28 '02 16:16:34 PST]
Print Job
Close

Figure 6-3: Job Details Window

4 Review the job

On the right-hand side of the window you can select tabs to view created, modified, and deleted objects in this job. Select the tab of interest, then select the object of interest by clicking on it. Selected details about the object will be displayed in the **Selected ... Detail**s panel. If you are examining a committed job that was rejected, you will find useful information in the **Job Results** tab.

5 Select Close

Select **Close** to close the window.

Delete Scheduled or Saved Jobs

You can delete jobs that have not yet been committed to the ISM Provision server, but once a job is committed it cannot be deleted. (Of course, you could review a committed job and reverse the individual changes you made, then commit.)

If you have access to the Network Infrastructure Manager client, there is a configuration versioning facility. You would probably want to create a configuration version if you think you might want to later remove a job you were planning to commit.

Steps. To delete a scheduled or saved job:

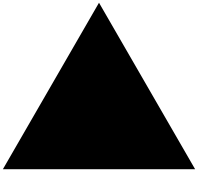
1 View the job in the Scheduled or Saved Jobs tab

See the task, “View Committed, Scheduled, or Saved Jobs”, if you need detailed instructions.

2 Select the Delete button

3 Select Delete to confirm, Cancel otherwise

When you selected the **Delete** button in step 2, a **Delete Job** window appears to confirm your choice. Select the **Delete** button on the window to delete the job.



Index

A

account password 2-3
add
- customer 5-3
- IP aggregation point 5-12
- IP range subscriber 5-9
- IP subscriber 5-7
- policy based service 4-7
- service bundle 4-4
- traffic policy 4-9

aggregation point 5-2

C

changes
- commit 6-1
- view 6-2

commit changes 6-1
conventions
- notice icons, Preface viii
- text, Preface viii

create
- customer 5-3
- IP aggregation point 5-12
- IP range subscriber 5-9
- IP subscriber 5-7
- policy based service 4-7
- service bundle 4-4
- traffic policy 4-9

customer 5-2
- add, create 5-3

D

Device Communicators 1-4
device communicators 1-4

I

icons, named 3-3
IP aggregation point 5-2
- add, create 5-12

IP range subscriber 5-2
- add, create 5-9

IP Service Manager 1-1, 1-5
IP subscriber 5-2
- add, create 5-7

IPSM client
- account password 2-3
- launch 2-2
- login 2-2
- user account 2-3

IPSM views
- selecting 3-2

ISM Provision 1-1
ISM Provision Server 1-4
ISM Provision server 1-4

J

job 6-1

K

key information 4-3

L

Launch
IPSM client 2-2
login 2-2
IPSM client 2-2

N

named icons 3-3
Network Infrastructure Manager 1-1, 1-5
NIM 1-5

P

policies
traffic 4-2
policy based service 4-2
add, create 4-7
policy based services 1-5
precedence 4-11
provider accounts 1-5
providers 1-5

S

saved jobs 6-2
selecting
IPSM views 3-2
server 1-4
service
add service bundle 4-4
bundle 4-2
category 4-3
policy based 4-2
Service Activation view 4-1, 5-1
service bundles 1-5
start 2-1
subscriber 5-2
subscribers 1-5
super-VLAN 5-2

T

traffic policies 4-2
traffic policy
add, create 4-9

U

user account 2-3
IPSM client 2-3

V

view
jobs 6-2
view changes 6-2
views
Service Activation 4-1, 5-1
VLAN
super, sub 5-2